Indian Journal of Modern Research and Reviews

This Journal is a member of the *'Committee on Publication Ethics'*

Online ISSN:2584-184X

Research Article

The Immunity-Disability Architecture of Digital Privacy: Reimagining Data Protection Rights Through Hohfeld's Analytical Framework

Soumyadip Panda [1*], Dr. Rupak Kr. Joshi [2]

[1] Research Scholar, School of Legal Studies, The Neotia University, West Bengal, India

[2] Assistant Professor, School of Legal Studies, The Neotia University, West Bengal, India

Corresponding Author: * Soumyadip Panda

DOI: https://doi.org/10.5281/zenodo.21508112

Abstract

Contemporary data protection law has largely conceptualised privacy as a bundle of subjective rights, enforceable through consent mechanisms, breach notification obligations, and supervisory authority sanctions. This framing, while practically important, obscures the deeper architectural structure of legal relations that governs the digital privacy domain. The present article argues that Wesley Newcomb Hohfeld's analytical jurisprudence — and specifically the immunity-disability correlative — provides a more precise and theoretically coherent vocabulary for understanding how constitutional and statutory privacy protections insulate data subjects from the legal power of both state and corporate actors. Drawing on doctrinal legal research, comparative constitutional analysis, and interpretive jurisprudential inquiry, the article reconstructs the major instruments of digital privacy law — the European Union's General Data Protection Regulation, constitutional privacy doctrines in India, the United States, and Germany, and emerging platform regulatory frameworks — through the lens of Hohfeldian legal relations. The central finding is that constitutional privacy protections are most accurately characterised as immunities structurally disabling state and corporate actors from altering the data subject's protected legal position without satisfying constitutionally mandated conditions. This reconceptualisation has significant implications for judicial reasoning, regulatory design, and the normative theory of informational self-determination in surveillance-intensive digital environments.

Manuscript Information

- **ISSN No:** 2584-184X
- **Received:** 12-06-2026
- **Accepted:** 20-07-2026
- **Published:** 23-07-2026
- **MRR:**4(7); 2026: 183-192

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Panda S, Joshi R Kr. The Immunity-Disability Architecture of Digital Privacy: Reimagining Data Protection Rights Through Hohfeld's Analytical Framework. Indian J Mod Res Rev. 2026;4(7):183-192.

Access this Article Online

www.mrrjournal.in

KEYWORDS: Hohfeldian jurisprudence; immunity-disability; digital privacy; data protection law; informational self-determination; constitutional rights; platform regulation

1. INTRODUCTION

The contemporary individual lives in a condition of continuous informational exposure. Every transaction, movement, communication, and expression of preference generates data that is captured, aggregated, inferred upon, and monetised by institutional actors whose analytical capacity vastly exceeds the individual's capacity to comprehend, let alone contest, what is being done with it. This asymmetry is not incidental to the digital economy; it is constitutive of it. Shoshana Zuboff has characterised the resulting formation as surveillance capitalism, a system in which human experience is claimed as free raw material for behavioural prediction and modification [15], while David Lyon's earlier account of the surveillance society had already identified the routinisation of monitoring as an ordinary feature of everyday administrative life [24]. The state, meanwhile, has not been displaced by the platform but has learned to operate alongside and through it, acquiring access to communications metadata, location histories, biometric identifiers, and behavioural profiles on a scale that the architects of twentieth-century constitutional privacy doctrine could not have anticipated.

Law has responded to this condition principally through the vocabulary of rights. The European Union's General Data Protection Regulation confers upon the data subject an elaborate catalogue of entitlements — access, rectification, erasure, portability, objection, and protection against solely automated decision-making [6]. Constitutional courts across jurisdictions have recognised privacy as a fundamental right: the Supreme Court of India in Justice K.S. Puttaswamy v. Union of India [20], the German Federal Constitutional Court in its informational self-determination jurisprudence [16], and the United States Supreme Court in its progressive digital reformulation of Fourth Amendment doctrine [12]. Scholarly treatment has largely followed suit, tracing a lineage from Warren and Brandeis's articulation of the right to be let alone [3] through Westin's reconceptualisation of privacy as control over the circulation of personal information [4]. The result is a rich but conceptually undifferentiated body of law and commentary in which the word 'right' performs a great deal of work without disclosing what kind of legal relation it denotes in any given instance.

This conceptual imprecision is the point of departure for the present article. More than a century ago, Wesley Newcomb Hohfeld demonstrated that the term 'right' conceals at least four analytically distinct legal relations — claim-right, privilege, power, and immunity — each with its own correlative and its own operative logic [1]. His central insight was that a great deal of legal confusion arises not from disagreement about values but from the conflation of relations that differ in kind. The distinction that matters most for present purposes is that between first-order relations, which govern conduct directly, and second-order relations, which govern the capacity to alter legal positions at all. A duty tells an actor what it must or must not do; a disability tells an actor what it cannot validly do, however it may in fact behave. The difference between these two is the difference between an act that is unlawful and remediable and an act that is void and without legal effect.

Once this distinction is brought to bear on digital privacy law, a significant analytical problem becomes visible. When a constitutional court strikes down a surveillance statute for infringing privacy, it is not ordinarily holding that the state has breached a duty owed to a particular citizen and must therefore compensate her. It is holding that the legislature lacked the constitutional competence to enact the measure at all. That is not the logic of a claim-right and a correlative duty; it is the logic of an immunity and a correlative disability. Yet the prevailing scholarship — including the substantial literature generated by the GDPR, the constitutional privacy jurisprudence of Germany and India, and the theoretical interventions of Balkin [27], Yeung [31], and Pasquale [32] — has not systematically reconstructed digital privacy protections in these terms. The immunity-disability correlative, the least examined of Hohfeld's four pairs, remains largely absent from a field in which it is arguably the most explanatory.

The consequences of this omission are not merely taxonomic. If constitutional and statutory privacy protections are properly characterised as immunities, then several doctrinal propositions follow that the claim-right framing obscures. Legislative acts that fail proportionality review are void as against the protected individual rather than merely unlawful. Absolute processing prohibitions, such as those governing special categories of data, operate as structural incapacities that no quantum of consent engineering or technical ingenuity can cure. Automated decisions taken in contravention of the applicable conditions are incapable of producing valid legal effects rather than being merely actionable after the fact. And the burden of establishing an enabling condition falls upon the actor asserting the power, rather than upon the individual who must otherwise first discover the intrusion, demonstrate harm, and initiate proceedings. The immunity framing, in short, relocates protection from the remedial stage to the constitutive stage — a shift of considerable practical significance for data subjects who, by hypothesis, rarely know what has been done with their information.

Accordingly, this article pursues three connected objectives. The first is analytical: to reconstruct Hohfeld's taxonomy with sufficient precision to distinguish the immunity-disability relation from the claim-right structure with which it is habitually conflated, and to establish the criteria by which the two may be identified in operative legal materials. The second is doctrinal and comparative: to map the principal instruments of digital privacy law — the GDPR and the Charter of Fundamental Rights, the German Basic Law as elaborated in Volkszählungsurteil and the IT-Grundrecht judgment, the Indian constitutional framework following Puttaswamy together with the Digital Personal Data Protection Act 2023 [42], and the American Fourth Amendment jurisprudence —

onto this reconstructed architecture, and to assess how completely each instantiates a genuine immunity structure. The third is diagnostic and prescriptive: to identify what the article terms the immunity deficit in the domain of corporate algorithmic power, where consequential decisions are taken over individuals without operating through any recognised legal power and therefore without attracting the immunity constraints that constitutional law imposes upon the state, and to consider what regulatory design would be required to close it.

The central claim advanced is that constitutional privacy protections are most accurately characterised as immunities that structurally disable state and corporate actors from altering the data subject's protected legal position without satisfying constitutionally mandated conditions — and that this characterisation, far from being a scholastic refinement, changes how courts should reason, how regulators should draft, and how the normative claim of informational self-determination should be understood in surveillance-intensive environments.

The article proceeds as follows. Section 2 surveys the existing literature on Hohfeldian jurisprudence, privacy theory, and comparative data protection constitutionalism, and locates the gap the article addresses. Section 3 sets out the doctrinal, jurisprudential, and comparative methodology employed and identifies the primary legal materials examined. Section 4 develops the conceptual and analytical framework, reconstructing Hohfeld's taxonomy and applying the immunity-disability correlative to constitutional privacy and to corporate data processing power. Section 5 presents the findings of the comparative doctrinal analysis, mapping the immunity architecture across the selected jurisdictions and examining state surveillance power and algorithmic decision-making in turn. Section 6 discusses the theoretical contributions, the implications for regulatory design, and the limitations of the framework, including the difficulties of transposing a taxonomy developed for private law into constitutional and regulatory contexts. Section 7 concludes.

2. LITERATURE REVIEW

The jurisprudential legacy of Wesley Newcomb Hohfeld occupies a foundational position in analytical legal philosophy. Published in the Yale Law Journal between 1913 and 1917, Hohfeld's celebrated taxonomy disaggregated the concept of a 'right' into eight irreducibly distinct legal relations organized in correlative and opposite pairs: rights and duties; privileges (liberties) and no-rights; powers and liabilities; and immunities and disabilities [1]. The significance of this taxonomy was not merely classificatory but explanatory: it revealed that much legal confusion arose from the conflation of relations that are analytically distinct. As Hohfeld demonstrated through careful examination of equity and property cases, a litigant's claim that she 'had a right' could mean any of at least four different things depending upon the relational context [1]. This insight, amplified by H.L.A. Hart's subsequent work on the concept of a legal right [2], became constitutive of much twentieth-century jurisprudence on rights theory.

Despite the enduring influence of Hohfeld's taxonomy in private law and constitutional theory, its application to the domain of data protection and digital privacy has remained underdeveloped. The foundational scholarship on privacy as a legal concept — from Warren and Brandeis's seminal 1890 article on the right to be let alone [3], through Alan Westin's reconceptualization of privacy as informational self-determination [4], and Paul Schwartz's analysis of privacy and democracy in cyberspace [5] — has generally proceeded within a rights-based framework that collapses the Hohfeldian distinctions. Westin's influential formulation, which grounded informational privacy in the individual's capacity to control personal data flows, implicitly invokes a claim-right structure but does not distinguish it from the immunity dimension that shields the individual from externally imposed modifications of her legal position [4]. This conflation, while perhaps harmless in contexts where the distinction between first-order and second-order legal relations is not practically significant, becomes analytically costly precisely where constitutional privacy is invoked as a constraint on legislative power.

The emergence of comprehensive data protection regimes, most significantly the European Union's General Data Protection Regulation (GDPR) of 2016 [6], has generated an enormous volume of legal scholarship. Paul De Hert and Serge Gutwirth's analysis of the interplay between privacy and data protection within the EU constitutional order [7] provided an important conceptual map, distinguishing privacy as a transparency tool from data protection as an opacity instrument. Brendan Van Alsenoy's comprehensive study of data protection law as a system of legal obligations [8] focuses on the controller-processor relationship and the liability framework without engaging whether the data subject's constitutionally grounded position is better understood as a Hohfeldian immunity against the exercise of legal power. Similarly, the extensive scholarship generated by the GDPR's extraterritorial application and Anu Bradford's analysis of the Brussels Effect [29] addresses regulatory power at the systemic level without examining the immunity-disability structure operative at the individual-state or individual-platform level.

The constitutional dimension of digital privacy has attracted substantial scholarship across multiple jurisdictions. In the United States, the evolution from the Fourth Amendment's property-based conception in Olmstead v. United States [9] through the penumbral theory in Griswold v. Connecticut [10], the reasonable expectation doctrine in Katz v. United States [11], and the digital-age reformulations in Carpenter v. United States [12] and Riley v. California [13] reflects a jurisprudential trajectory in which constitutional privacy protection has progressively acquired immunity-like characteristics. Neil Richards's analysis of surveillance dangers [14] and Shoshana Zuboff's theoretical work on surveillance capitalism [15] have illuminated the structural power asymmetries between data subjects and corporate platforms, but neither has subjected

these asymmetries to systematic Hohfeldian analysis, leaving a significant theoretical gap that the present article seeks to fill.

The German constitutional tradition provides perhaps the most sophisticated elaboration of privacy as a structural immunity. The Federal Constitutional Court's landmark Volkszählungsurteil decision of 1983, which articulated the right to informational self-determination under the Basic Law [16], established that individuals possess a constitutionally protected interest in the control of their personal data that constrains both state and, through mittelbare Drittwirkung, private actors. The subsequent IT-Grundrecht judgment of 2008 [17] recognized a constitutional right to confidentiality and integrity of information technology systems. Christoph Gusy and Kai von Lewinski's analysis of German data protection constitutionalism [18] and Spiros Simitis's foundational work on informational self-determination [19] have explored these doctrines without situating them within the Hohfeldian analytical structure — an oversight that limits the comparative utility of this otherwise rich body of scholarship.

In India, the Supreme Court's unanimous judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India [20] recognized privacy as a fundamental right under Article 21 of the Constitution. Scholars including Usha Ramanathan [21] and Vrinda Bhandari [22] have examined the implications of this judgment for data governance, while Rishab Bailey and Smriti Parsheera [23] have analyzed the subsequent Personal Data Protection framework. The question of whether the constitutional privacy right in India operates as a Hohfeldian immunity — disabling the state from legislating data-intrusive measures without satisfying the proportionality test — has not, however, been systematically addressed in this literature. The surveillance studies scholarship of David Lyon [24] and Mark Andrejevic [25], together with Julie Cohen's theory of the biopolitical public domain [26] and Jack Balkin's theory of information fiduciaries [27], provide important normative context but do not engage the second-order relational structure that the immunity-disability framework illuminates. Christopher Kuner's work on transborder data flows [30], Karen Yeung's analysis of algorithmic regulation [31], and Frank Pasquale's examination of the black box society [32] each identify structural power asymmetries in the digital environment that the Hohfeldian framework is uniquely positioned to analyze with analytical precision.

3. RESEARCH METHODOLOGY

This article adopts a doctrinal jurisprudential methodology informed by comparative constitutional analysis and interpretive legal reasoning. Doctrinal legal research, as the primary methodological approach, involves the systematic examination, interpretation, and conceptual reconstruction of primary legal materials — constitutional texts, statutory instruments, judicial decisions, regulatory guidance, and international legal instruments — with a view to identifying and articulating the underlying legal principles and the structural relations they instantiate [33]. The doctrinal method is appropriate here because the research question is fundamentally one of legal classification and analytical reconstruction: whether the immunity-disability structure in Hohfeld's taxonomy more accurately describes the legal position of data subjects in constitutional and statutory frameworks than the claim-right structure conventionally employed.

The jurisprudential method employed throughout is analytical rather than primarily critical or sociological. Following the tradition of analytical jurisprudence associated with Bentham, Austin, Hart, Hohfeld, and Raz, the article seeks to clarify the conceptual structure of legal relations in the digital privacy domain [34]. Albert Kocourek's elaboration of Hohfeld's system [35] and Tony Honoré's application of the framework to property law [36] provide methodological precedents for this kind of conceptual reconstruction. The comparative constitutional method examines privacy jurisprudence across three major constitutional systems — the United States, Germany, and India — selected because they represent distinct constitutional traditions and have each generated influential doctrinal frameworks for digital privacy: the American tradition grounds privacy in a negative liberty against state intrusion through the Fourth Amendment; the German tradition grounds it in an affirmative constitutional right to informational self-determination under the Basic Law; and the Indian tradition represents a synthesis incorporating elements of both.

Primary legal materials examined include: the EU General Data Protection Regulation (Regulation (EU) 2016/679) and the Charter of Fundamental Rights; the Indian Constitution and the Digital Personal Data Protection Act 2023; the United States Constitution (Fourth and Fourteenth Amendments), the Electronic Communications Privacy Act, and the California Consumer Privacy Act; the German Basic Law and the Federal Data Protection Act; United Nations General Assembly resolutions on the right to privacy in the digital age; and the Council of Europe's Convention 108+. Judicial authorities examined include decisions of the Court of Justice of the European Union (Schrems I and Schrems II), the German Federal Constitutional Court (Volkszählungsurteil, IT-Grundrecht, and the BND Reform Act case), the United States Supreme Court (Carpenter, Riley, Katz), and the Supreme Court of India (Puttaswamy). No empirical methods, quantitative analyses, simulation techniques, or computational approaches are employed; the analysis is entirely interpretive and conceptual, as befits a paper of doctrinal jurisprudential character.

4. Conceptual and Analytical Framework

4.1 Reconstructing Hohfeld's Taxonomy

Before applying Hohfeld's analytical framework to the digital privacy domain, it is necessary to reconstruct its essential architecture with some precision, since popular usage has frequently conflated the relations in ways that Hohfeld himself specifically criticized. Hohfeld identified four pairs of jural correlatives — relations between two parties such that the existence of one necessarily entails the existence of the other in the correlative position — and four pairs of jural opposites —

relations such that the existence of one necessarily excludes the other for the same party in the same context [1]. The four correlative pairs are: (1) right (claim-right) and duty; (2) privilege (liberty) and no-right; (3) power and liability; and (4) immunity and disability.

The most important distinction for present purposes is between first-order and second-order legal relations. The right-duty and privilege-no-right pairs constitute first-order relations in that they directly govern permissible conduct. A data subject who has a claim-right that her controller not process her data without lawful basis occupies a different legal position from one who merely has a liberty to withhold consent: the former imposes a correlative duty on the controller; the latter means only that the data subject faces no duty to share. The power-liability and immunity-disability pairs are, by contrast, second-order relations: they govern not conduct directly but the capacity to alter legal relations. A power is a legally recognized capacity to change one's own or another's legal position; its correlative, liability, is the susceptibility of having one's legal position changed. An immunity is the absence of liability: the condition of being legally protected against having one's legal position changed by another actor's purported exercise of power. A disability is the correlative of immunity: the incapacity to alter another's legal position in a specific respect, regardless of the actor's factual capability [1]. Figure 1 below presents the complete Hohfeldian architecture as applied to the digital privacy domain.

HOHFELDIAN LEGAL RELATIONS IN DIGITAL PRIVACY		
FIRST-ORDER RELATIONS (Conduct Level)	**SECOND-ORDER RELATIONS (Power Level)**	**CORRELATIVES & OPPOSITES (Structural Logic)**
Right (Claim-Right) Data Subject vs. Controller GDPR Arts. 15-22	Power Legislative / DPA Authority to create/alter legal relations	Right <-> Duty Privilege <-> No-Right Power <-> Liability Immunity <-> Disability
Privilege (Liberty) Controller's processing authority; Art. 6 lawful bases	Liability Controller susceptible to DPA orders / void acts	IMMUNITY ARCHITECTURE Constitutional shield against unauthorized state/corporate power
DISABILITY ARCHITECTURE | State and Corporate Actors: Legally incapacitated from altering data subject's immunity-protected legal position | Unauthorized acts void, not merely unlawful		

Figure 1: See Diagram Below

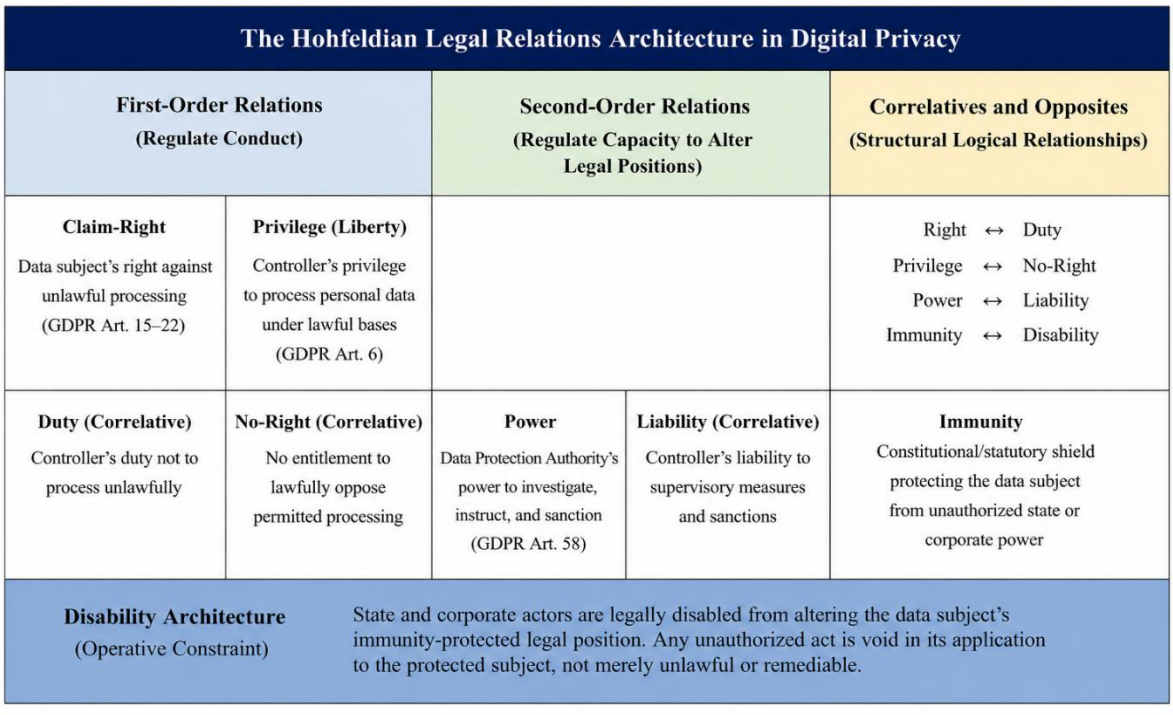

Figure 1: The Hohfeldian Legal Relations Architecture in Digital Privacy

4.2 Constitutional Privacy as Immunity

The reconceptualisation of constitutional privacy as an immunity structure resolves a persistent ambiguity in privacy jurisprudence concerning what it means for a constitutional court to uphold a privacy right against legislation. When courts hold that a state surveillance law is unconstitutional because it violates the right to privacy, they are not holding that the state has breached a duty correlative to the citizen's claim-right in the ordinary first-order sense. Constitutional invalidation operates at the second-order level: the legislature is found to have

exceeded its constitutionally delimited power. The citizen's constitutional privacy protection, properly analyzed, is an immunity against the exercise of state power over her privacy-related legal position, and the legislature's incapacity to override this immunity without satisfying proportionality conditions is a disability in the Hohfeldian sense. The practical consequence is that the offending legislative act is legally void — of no effect — rather than merely unlawful and remediable in damages.

This analysis is confirmed by the structure of proportionality review as employed by constitutional courts in the digital privacy domain. When the German Federal Constitutional Court examined the population census legislation in Volkszählungsurteil, it held that the constitutional right to informational self-determination imposed structural limits on the legislature's power to authorize data collection, and that the legislation failed to satisfy those limits [16]. The court's reasoning tracks the Hohfeldian immunity analysis precisely: the individual's immunity means that the legislature is disabled from enacting data-intrusive legislation unless the proportionality conditions of legitimate purpose, necessity, and appropriateness are met. Where those conditions are not met, the legislative act is constitutionally void as against the individual's protected position. The same logic structures the CJEU's analysis in Schrems I and Schrems II, where the Court of Justice invalidated the Safe Harbour and Privacy Shield adequacy decisions on the grounds that they failed to guarantee protection essentially equivalent to that provided under EU law [37][38]. EU citizens' Charter rights to privacy and data protection constitute an immunity that disables both EU institutions and member states from transferring personal data to third countries whose legal systems do not provide equivalent protection.

4.3 Corporate Data Processing Power and the Disability Architecture

The immunity-disability architecture also illuminates the relationship between data subjects and corporate data processors in ways that the conventional claim-right framing does not capture with full analytical precision. When a data subject exercises her right to erasure under Article 17 of the GDPR, she is not merely making a claim that the controller breaches a duty if it refuses; she is, in the Hohfeldian second-order sense, exercising a power to alter her legal relationship with the controller by withdrawing the lawful basis for processing. The correlative of this power is the controller's liability — its susceptibility to having the legal basis for processing altered. Where the GDPR imposes absolute prohibitions on certain categories of processing — special category data under Article 9 — it effectively creates a domain of disability for the controller: the controller lacks the legal power to render such processing lawful regardless of the technical or commercial means deployed. The controller's incapacity here is not remediable by enhanced consent mechanisms or technical workarounds; it is a structural legal disability attaching to the category of data and the nature of the processing.

The disability framing is particularly illuminating in the context of algorithmic decision-making under Article 22 of the GDPR, which restricts automated decisions that produce legal or similarly significant effects. Article 22 can be reconstructed as a structural disability imposed on controllers that operate automated decision-making systems: they are legally incapacitated from rendering automated decisions valid against the data subject without meeting the conditions specified in Article 22(2). If Article 22 creates an immunity and correlative disability rather than merely a claim-right and correlative duty, then automated decisions made in violation of Article 22 are legally void as against the data subject rather than merely actionable for compensation. This distinction matters practically and normatively: the immunity framing is more protective because it does not require the data subject to discover the violation, sustain demonstrable harm, and initiate enforcement proceedings; legal invalidity attaches automatically.

5. FINDINGS AND ANALYSIS

5.1 Mapping the Hohfeldian Architecture Across Major Frameworks

The doctrinal examination of constitutional and statutory privacy frameworks across the three comparator jurisdictions reveals a consistent, if not uniformly articulated, immunity-disability architecture underlying the major instruments of digital privacy protection. Table 1 below presents a comparative mapping of the primary legal relations operative in each framework, distinguishing between the conventional claim-right interpretation and the Hohfeldian immunity interpretation, and identifying the corresponding disability that each immunity entails.

Table 1: Comparative Hohfeldian Analysis of Major Digital Privacy Frameworks

Jurisdiction / Instrument	Conventional Rights Framing	Hohfeldian Immunity Framing	Corresponding Disability
EU GDPR (2016) / Charter Arts. 7-8	Data subject's right to access, erasure, portability; controller's duty to comply upon request	Data subject's immunity against unauthorized alteration of processing lawfulness by the controller or institution	Controller disabled from creating valid lawful basis outside Art. 6 grounds; adequacy decisions void if immunity conditions unmet (Schrems I & II)
Germany — Volkszahlungsurteil (1983) / IT-Grundrecht (2008)	Positive right to informational self-determination under Basic Law Arts. 2(1) / 1(1); constitutional right to IT system integrity	Individual's constitutional immunity against state legislative/executive data collection and surveillance powers	Legislature disabled from enacting data-collection statutes failing proportionality review; such statutes are constitutionally void, not merely unlawful

India — Puttaswamy (2017); DPDPA 2023	Fundamental right to privacy under Art. 21; statutory rights to correction and erasure	Immunity grounded in Art. 21's dignity core against surveillance legislation and corporate processing without lawful basis	State disabled from authorizing surveillance without proportionality; processing without lawful basis creates a power vacuum, not just a remediable duty breach
USA — Fourth Amendment / Carpenter / Riley	Negative liberty; reasonable expectation of privacy; exclusionary rule as remedy for state violation	Structural immunity of digital data against warrantless state access; third-party doctrine as immunity-limiting rule reducing scope of protection	State actors disabled from compelling production of content-layer digital data without warrant satisfying particularity; third-party doctrine contracts but does not eliminate the disability
CCPA / California Privacy Rights Act	Consumer rights to know, delete, opt-out; business obligations to honor rights requests	Partial immunity: consumer can disable business processing by exercising opt-out power; weaker than GDPR immunity structure	Business disability to sell personal data activated only by consumer's opt-out exercise; not a comprehensive immunity since lawful bases for processing remain broad absent opt-out

Table 1 reveals several significant analytical findings. First, the immunity-disability framing is substantially more coherent than the claim-right framing as a description of constitutional privacy protections, because constitutional invalidation of legislation is structurally an immunity-based operation rather than a duty-breach remedy. Second, the degree of immunity protection varies significantly across jurisdictions: the German and EU frameworks provide the most robust immunity architecture, grounded in constitutional norms that disable both state and corporate actors from creating valid legal bases for privacy-intrusive data use outside constitutionally specified conditions. The American framework provides a narrower immunity focused on state actors through the Fourth Amendment but substantially contracts the immunity through the third-party doctrine, which treats voluntarily shared data as falling outside the immunity's operative scope. The Indian framework, following Puttaswamy, provides a structurally strong immunity rooted in Article 21's inviolable dignity core but has not yet developed the institutional infrastructure to enforce the corresponding disabilities against corporate actors at scale. Third, the CCPA provides only partial immunities: it empowers consumers to exercise opt-out powers but does not structurally disable businesses from processing personal data in the way GDPR Article 9 disables controllers from processing special category data absent explicit consent or another Article 9(2) ground.

5.2 Surveillance Power, State Disability, and Legislative Competence

The immunity-disability framework provides particularly sharp analytical purchase in the context of state surveillance powers. Legislative authorization of surveillance involves the exercise of legislative power to create a legal framework within which executive actors may intrude upon individual privacy. If the individual's constitutional privacy protection is an immunity, then any legislative act that purports to authorize surveillance must clear the threshold imposed by the immunity's conditions; a legislative act that fails to satisfy those conditions is not merely unlawful but legally void in its application to the immunity-protected individual. This transforms the doctrinal question from 'has the state breached its duty?' to 'did the legislature possess the power to authorize this intrusion?' — a question that engages the ultra vires dimension of administrative and constitutional law rather than merely the remedial dimension.

This analysis generates a finding of practical importance: the doctrinal debate about whether surveillance legislation 'violates' a privacy right is misdescribed as a question of breach when it is more accurately a question of legislative competence. The German Constitutional Court's treatment of the BND Reform Act [39] and the Court of Justice's analysis of the national security exceptions under the ePrivacy Directive in La Quadrature du Net [40] both implicitly adopt this ultra vires framing. The immunity analysis makes the structural logic explicit: where constitutional proportionality conditions are not met, the state not only acts unlawfully but acts in excess of its constitutionally defined power, and the affected individual's immunity means that no valid legal effect is created against her protected position. This has consequences for the allocation of enforcement burdens: in a disability-based framework, the state must establish the existence of an enabling condition before the intrusive act takes legal effect, rather than the individual bearing the burden of challenging a presumptively valid act after the fact.

5.3 Algorithmic Power and the Immunity Deficit

The most significant immunity deficit identified by the doctrinal analysis concerns algorithmic decision-making systems operated by private corporations. Automated systems that profile individuals, allocate creditworthiness, determine social media visibility, assign insurance risk categories, or influence access to employment create significant effects on individuals' legal and material positions. Yet, as Karen Yeung has observed [31], these systems operate largely outside the traditional frameworks of legal power and accountability because they are neither legislative acts nor judicial decisions in the formal sense. Frank Pasquale's examination of the opacity of algorithmic systems [32] identifies the practical dimensions of this deficit without the Hohfeldian vocabulary to articulate its structural character.

From the Hohfeldian perspective, this observation can be sharpened into a structural claim: algorithmic decision-making systems exercise de facto power over individuals without the corresponding legal structure of power-liability-immunity-disability that governs formal legal institutions. When a credit-scoring algorithm determines that an individual is ineligible for

a mortgage, it produces an effect on her legal and material situation without operating through any recognized legal power in the formal sense. The individual has no immunity in the technical Hohfeldian sense against this exercise of de facto power because immunity operates specifically against legally recognized powers; it does not protect against factual capacity exercised outside any legal framework. This is the immunity deficit: the absence of a legal structure that would subject algorithmic power to the immunity constraints that constitutional law imposes on state power. GDPR Article 22 and the EU Artificial Intelligence Act [41] represent attempts to close this deficit by creating partial disabilities for deployers of consequential automated systems, but as the analysis in Section 3.3 established, Article 22's architecture remains incomplete because it does not render unauthorized automated decisions void ab initio.

6. DISCUSSION

6.1 Theoretical Contributions to Privacy Scholarship

The immunity-disability architecture of digital privacy developed in this article makes several distinct theoretical contributions. The most fundamental is the demonstration that constitutional privacy protections are structurally immunities rather than claim-rights, and that this difference in legal type has concrete analytical, doctrinal, and institutional consequences. The immunity framing explains why constitutional privacy protections operate as constraints on legislative power rather than merely as grounds for individual remedies; why their violation renders legislative acts void rather than merely unlawful; and why proportionality review in constitutional privacy cases is more accurately understood as a test of whether the legislative disability can be displaced by a constitutionally recognized enabling condition rather than as a balancing of competing rights. This reframing has the further advantage of generating a more coherent account of the relationship between individual privacy rights and structural institutional design: privacy-as-immunity is a feature of the constitutional architecture that limits the scope of institutional power, not merely a subjective entitlement that individuals must assert through litigation.

The framework also contributes to the literature on the relationship between privacy law and legal power. Jack Balkin's information fiduciary theory [27] imposes trust obligations on platforms but does not systematically address the power-liability-immunity-disability structure. The immunity-disability framework complements the fiduciary approach: the platform-as-fiduciary is disabled from exercising its data-processing powers in ways that conflict with the beneficiary's protected interests, and the beneficiary's immunity means that purported exercises of such power do not create valid legal effects against her protected position. This integration provides a more complete account of the structural relations between platforms and users. Moreover, the immunity-deficit finding in the algorithmic domain connects with Yeung's regulatory critique [31] and Pasquale's transparency argument [32] by identifying the precise legal-structural mechanism through which algorithmic power escapes conventional accountability: it operates outside the power-immunity-disability structure that would subject it to constitutional and regulatory constraint.

6.2 Implications for Regulatory Design

The immunity-disability architecture carries significant prescriptive implications for the design of data protection regulation. If the normative goal of data protection law is to protect individuals against illegitimate exercises of power over their informational autonomy, then regulatory frameworks should be designed to create genuine legal disabilities for controllers and processors rather than merely to impose duties that generate liability upon breach. The difference is between regulatory provisions that render unauthorized data use legally void as against the data subject and provisions that render it merely actionable for compensation or supervisory sanction. The former architecture is more protective because it does not require the data subject to discover the violation and initiate enforcement proceedings; the invalidity of the unauthorized processing attaches automatically and operates against the controller regardless of whether the data subject is aware of the intrusion. Accordingly, for policymakers designing the next generation of digital privacy frameworks — including the EU Data Act, the proposed American Data Privacy and Protection Act, and India's Digital Personal Data Protection Act 2023 [42] — the immunity analysis suggests that the most robust provisions are those that create clear disabilities: absolute prohibitions on certain categories of processing that render unauthorized acts void rather than merely prohibited.

6.3 Limitations and Countervailing Considerations

The immunity-disability framework is not without limitations. The most significant is that Hohfeld's analytical jurisprudence, developed primarily in the context of private law relationships between identified parties, must be adapted to the constitutional and regulatory context in which the relevant legal relations obtain between individuals and institutional actors of vastly different resources and capabilities. The concept of disability requires careful specification in each context: a legislative disability means that legislation is constitutionally void; an administrative disability means that administrative action is ultra vires; and a corporate disability in the data protection context means that data processing creates no valid legal effect against the protected individual. These are structurally analogous but institutionally distinct applications of the disability concept, and the transitions between them require normative justification that the purely analytical Hohfeldian framework does not itself supply.

A further limitation concerns the enforceability of immunities against corporate actors in the absence of effective constitutional horizontal effect. While the German doctrine of mittelbare Drittwirkung and the GDPR's direct applicability to private controllers provide mechanisms through which the immunity architecture can constrain corporate power, the American constitutional framework, grounded in state action doctrine, provides constitutional immunities only against

government actors. The immunity deficit identified in Section 4.3 is therefore most acute in the American regulatory context, where comprehensive federal data protection legislation has not been enacted. This limitation points to the importance of legislative action to supply the disability architecture that constitutional law does not, in that jurisdiction, provide directly — and suggests that the Hohfeldian framework can serve a diagnostic as well as a descriptive function, identifying structural lacunae in privacy protection that require legislative remedy.

7. CONCLUSION

This article has demonstrated that Hohfeld's analytical jurisprudence — specifically the immunity-disability correlative — provides a more precise and theoretically coherent framework for understanding constitutional and statutory digital privacy protections than the claim-right framing that dominates existing scholarship. By reconstructing major privacy instruments including the GDPR, the German Basic Law's informational self-determination jurisprudence, the Indian Puttaswamy framework, and the American Fourth Amendment digital privacy doctrines through the Hohfeldian analytical lens, the article has shown that constitutional privacy protections are most accurately understood as immunities structurally disabling state and corporate actors from altering the data subject's protected legal position without satisfying constitutionally mandated enabling conditions. This reconceptualization carries concrete doctrinal consequences: constitutional invalidation of surveillance legislation operates as a disability-based void rather than a duty-breach remedy; GDPR Article 9 absolute prohibitions create genuine controller disabilities rather than mere obligatory duties; and Article 22's automated decision-making restrictions approach, without fully instantiating, a genuine immunity architecture. The immunity deficit identified in the context of corporate algorithmic power reveals the structural incompleteness of existing frameworks and points to the need for regulatory design that creates genuine legal disabilities for deployers of consequential automated systems. Future scholarship should examine whether the EU AI Act, the Digital Personal Data Protection Act 2023, and proposed American federal privacy legislation sufficiently close this immunity deficit, and whether the immunity-disability framework can be extended to address emerging challenges of biometric surveillance, real-time profiling, and cross-border data flows. The Hohfeldian vocabulary developed here provides the analytical foundation for that inquiry.

REFERENCES

1. Hohfeld WN. Some fundamental legal conceptions as applied in judicial reasoning. Yale Law J. 1913;23(1):16-59. doi:10.2307/785533.
2. Hart HLA. *Essays on Bentham: Studies in Jurisprudence and Political Theory*. Oxford: Oxford University Press; 1982.
3. Warren SD, Brandeis LD. The right to privacy. Harv Law Rev. 1890;4(5):193-220. doi:10.2307/1321160.
4. Westin AF. *Privacy and Freedom*. New York: Atheneum; 1967.
5. Schwartz PM. Privacy and democracy in cyberspace. Vand Law Rev. 1999;52(6):1609-1702.
6. European Parliament and Council. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Off J Eur Union. 2016;L119:1-88.
7. De Hert P, Gutwirth S. Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action. In: Gutwirth S, et al., editors. *Reinventing Data Protection?* Dordrecht: Springer; 2009. p. 3-44.
8. Van Alsenoy B. *Data Protection Law in the EU: Roles, Responsibilities and Liability*. Cambridge: Intersentia; 2019.
9. *Olmstead v. United States*. 277 U.S. 438 (1928).
10. *Griswold v. Connecticut*. 381 U.S. 479 (1965).
11. *Katz v. United States*. 389 U.S. 347 (1967).
12. *Carpenter v. United States*. 585 U.S. 296 (2018).
13. *Riley v. California*. 573 U.S. 373 (2014).
14. Richards NM. The dangers of surveillance. Harv Law Rev. 2013;126(7):1934-65.
15. Zuboff S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs; 2019.
16. Bundesverfassungsgericht. *Volkszählungsurteil*, BVerfGE 65, 1 (Population Census Case). Federal Constitutional Court of Germany; 1983.
17. Bundesverfassungsgericht. BVerfGE 120, 274 (IT-Grundrecht). Federal Constitutional Court of Germany; 2008.
18. Gusy C, von Lewinski K. *Datenschutzrecht im Wandel: Grundlagen und Entwicklungen*. Baden-Baden: Nomos; 2015.
19. Simitis S. Reviewing privacy in an information society. Univ Pa Law Rev. 1987;135(3):707-46. doi:10.2307/3311925.
20. *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.* (2017) 10 SCC 1 (Supreme Court of India).
21. Ramanathan U. A unique identity bill. Econ Polit Wkly. 2010;45(30):10-14.
22. Bhandari V. Privacy as constitutional culture. Indian Law Rev. 2020;4(1):16-37. doi:10.1080/24730580.2020.1726956.
23. Bailey R, Parsheera S. *Data Localisation in India: Questioning the Means and Ends*. NIPFP Working Paper No. 242. New Delhi: National Institute of Public Finance and Policy; 2018.
24. Lyon D. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press; 2001.
25. Andrejevic M. *iSpy: Surveillance and Power in the Interactive Era*. Lawrence: University Press of Kansas; 2007.
26. Cohen JE. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven: Yale University Press; 2012.

27. Balkin JM. Information fiduciaries and the First Amendment. UC Davis Law Rev. 2016;49(4):1183-1234.
28. Determann L. *Determann's Field Guide to Data Privacy Law*. 4th ed. Cheltenham: Edward Elgar Publishing; 2020.
29. Bradford A. *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press; 2020.
30. Kuner C. *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press; 2013.
31. Yeung K. Algorithmic regulation: A critical interrogation. Regul Gov. 2018;12(4):505-23. doi:10.1111/rego.12158.
32. Pasquale F. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge (MA): Harvard University Press; 2015.
33. Hutchinson T, Duncan N. Defining and describing what we do: Doctrinal legal research. Deakin Law Rev. 2012;17(1):83-119. doi:10.21153/dlr2012vol17no1art70.
34. Raz J. *Ethics in the Public Domain: Essays in the Morality of Law and Politics*. Oxford: Oxford University Press; 1994.
35. Kocourek A. Various definitions of jural relations. Columbia Law Rev. 1920;20(4):394-412. doi:10.2307/1111118.
36. Honore AM. Ownership. In: Guest AG, editor. *Oxford Essays in Jurisprudence*. Oxford: Oxford University Press; 1961. p. 107-147.
37. *Case C-362/14, Schrems v. Data Protection Commissioner (Schrems I)*, ECLI:EU:C:2015:650 (Court of Justice of the European Union; 2015).
38. *Case C-311/18, Data Protection Commissioner v. Facebook Ireland (Schrems II)*, ECLI:EU:C:2020:559 (Court of Justice of the European Union; 2020).
39. Bundesverfassungsgericht. BVerfGE 154, 152 (BND Reform Act). Federal Constitutional Court of Germany; 2020.
40. *Case C-511/18, La Quadrature du Net v. Premier ministre*, ECLI:EU:C:2020:791 (Court of Justice of the European Union; 2020).
41. European Parliament and Council. Regulation (EU) 2024/1689 (Artificial Intelligence Act). Off J Eur Union. 2024; L1689.
42. Ministry of Electronics and Information Technology, Government of India. *The Digital Personal Data Protection Act, 2023*. New Delhi: Gazette of India; 2023.

About the Corresponding Author

Soumyadip Panda is a Research Scholar at the School of Legal Studies, The Neotia University, West Bengal, India. His academic interests include contemporary legal issues, constitutional law, human rights, and interdisciplinary legal research. He is committed to advancing legal scholarship through rigorous research and contributing to discussions on law, justice, and public policy.